Elluminate Feature Report

Feature Name: HTTP Tunneling

Internet Firewalls

The Internet protocol provides for over 65,000 possible connection “ports” for each unique network IP address on a Local Area Network (LAN). Firewalls protect LANs by blocking connections through arbitrary ports to external IP addresses. Firewalls permit and route external connections on specific ports to the appropriate LAN servers (Web, email, Elluminate, etc.). Firewalls sometimes allow arbitrary outbound connections, but more often block them. This is usually done to prevent computers infected by viruses from making external or backdoor connections. Sometimes firewalls are configured allow only selected outbound connections. For instance, port 80 and 443 traffic could be enabled to allow HTTP traffic, enabling Web browsing. If all connections are blocked, Web browsing is done through HTTP and HTTPS proxy servers, which enforce the use of specific ports and protocols.

Customer Problem

A connection to an Elluminate *Live!* session requires a direct TCP/IP connection, using a proprietary application protocol, from the client machine to the Elluminate server. The Elluminate server is configured to accept inbound connections on ports 2187, 80 and 443. Port 2187 is often one of the outbound ports that firewalls block. Ports 80 and 443 are usually configured for HTTP traffic, and may not accept connections in a proprietary application protocol. The result is that users behind enterprise firewalls often cannot connect to the Elluminate server to initiate an Elluminate *Live!* session.

Solution: HTTP Tunneling

Elluminate’s servers now feature HTTP Tunneling, which allows TCP/IP connections to Elluminate servers, and configured in our proprietary application protocol, through ports configured for HTTP traffic. Elluminate’s protocol is layered into HTTP allowing connections through standard enabled HTTP ports on networks and proxies. This process is referred to as HTTP Tunneling or HTTP Masking, and should work even if client machines have access to the Internet restricted by HTTP proxy servers.

Solution Restrictions:

- Successful HTTP Tunneling may require some manual configuration. Java Web Start should automatically detect an HTTP proxy, but if it cannot users may be required to enter proxy information directly into Java Web Start or Elluminate *Live!.*
- While the HTTP Tunneling feature greatly improves the likelihood of successful connection between the client and the server, it does not address:
    - Locked down PCs that are unable to install Java Web Start
    - Proxy firewalls that block Java Resource (JAR) files

Availability

Elluminate’s servers now feature HTTP Tunneling. HTTP Tunneling is available for deployment to Server clients.

Contact Information

For more information, contact Elluminate’s Services Team at support@elluminate.com.